

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

***This Page Blank (uspto)***

ABSTRACTED-PUB-NO: JP09009241A

BASIC-ABSTRACT:

The system has an adder (2) that adds the program classification data that indicates a program. A decoding data decodes the scramble data enciphered by a related data sending circuit (4). A predetermined contract data is output by a scramble C-system (6). The scramble

C-system controls the contract data from being sent to a receiving terminal provided with broadcast feed side. The contract data is stored

by a security module (9). The security module extracts the scramble data added to the program from the broadcast feed side.

A decoder (8) decodes the scramble data based on the decoding data stored by the memory. The security module judges the authenticity of the program. A predetermined audio and video data relating to the program indicated by a descrambler is offered by the security module.

ADVANTAGE - Quickly offers broadcast feed side with satisfactory audio and video data.

CHOSEN-DRAWING: Dwg. 1/5

TITLE-TERMS: SCRAMBLE DATA BROADCAST SYSTEM CHARGE BROADCAST  
SYSTEM SECURE MODULE OFFER PREDETERMINED AUDIO VIDEO DATA  
RELATED DATA

INDICATE DESCRAMBLER

This Page Blank (uspto)

特開平 9 - 9 2 4 1

(43) 公開日 平成 9 年 (1997) 1 月 10 日

(51) Int. Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H04N 7/167			H04N 7/167	
H04H 1/00			H04H 1/00	F
				N
H04N 7/16			H04N 7/16	C

審査請求 未請求 請求項の数 16 O L (全 11 頁)

(21) 出願番号 特願平 7 - 1 4 8 5 1 2

(22) 出願日 平成 7 年 (1995) 6 月 15 日

(71) 出願人 0 0 0 0 0 2 1 8 5

ソニー株式会社

東京都品川区北品川 6 丁目 7 番 3 5 号

(72) 発明者 山下 雅美

東京都品川区北品川 6 丁目 7 番 3 5 号 ソ  
ニー株式会社内

(72) 発明者 吉田 洋之

東京都品川区北品川 6 丁目 7 番 3 5 号 ソ  
ニー株式会社内

(72) 発明者 城間 真

東京都品川区北品川 6 丁目 7 番 3 5 号 ソ  
ニー株式会社内

(74) 代理人 弁理士 稲本 義雄

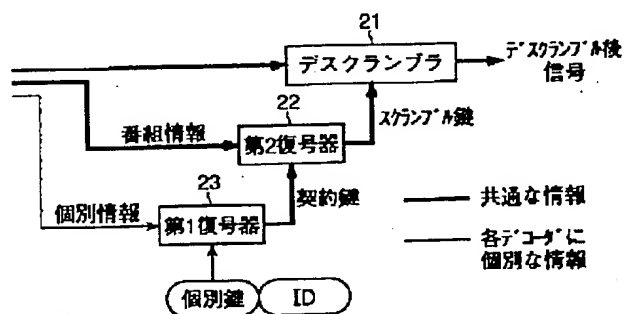
最終頁に続く

(54) 【発明の名称】 スクランプル放送システム、およびスクランブル方法、並びにスクランブル装置、およびデスクランブル装置

## (57) 【要約】

【目的】 有料放送の契約形態に拘らず、視聴制御を行うことができるようにする。

【構成】 放送供給側から、予め、所定の番組に対応する暗号化された契約鍵が個別情報に含めて受信端末に供給され、受信端末において、第 1 復号器 23 によって、受信端末固有の個別鍵によりこの契約鍵が復号される。受信端末に対して所定の操作が行われたとき、第 2 復号器 22 において、復号された契約鍵を用いてその番組に付加された番組情報の中のスクランブル鍵が復号され、デスクランブラ 21 に供給され、デスクランブラ 21 においてその番組がデスクランブルされる。また、放送供給側に対しては、その番組の視聴を行ったことが通知される。



## 【特許請求の範囲】

【請求項 1】 放送供給側から送信されてきたスクランブルされた所定のチャンネルの番組を、視聴者側の受信端末で受信し、受信した前記番組をデスクランブルするスクランブル放送システムにおいて、

前記放送供給側は、

スクランブルされた前記番組をデスクランブルするためのスクランブル情報を暗号化する暗号化手段と、

暗号化された前記スクランブル情報、および前記番組が特別番組であるか否かを示す番組種別情報を前記番組に付加する付加手段と、

前記暗号化手段により暗号化された前記スクランブル情報を復号する復号情報、および契約形態に対応する所定の契約情報を出力する出力手段と、

前記出力手段からの前記復号情報、および前記契約情報を前記受信端末に供給するか否かを制御する制御手段とを備え、

前記受信端末は、

前記放送供給側からの前記復号情報、および契約情報を記憶する記憶手段と、

前記放送供給側からの前記番組に付加された前記スクランブル情報を抽出する抽出手段と、

前記スクランブル情報を前記記憶手段に記憶された前記復号情報に基づいて復号する復号手段と、

前記番組のデスクランブルを行うか否かを指示する指示手段と、

前記番組種別情報に基づいて、前記番組が特別番組であるか否かを判定する判定手段と、

前記指示手段による指示内容、前記契約情報、および前記判定手段の判定結果に基づいて、前記番組を前記復号手段により復号された前記スクランブル情報を用いてデスクランブルするか否かを決定する決定手段と、

前記指示手段によって指示された番組に関する所定の視聴情報を前記放送供給側に提供する提供手段とを備えることを特徴とするスクランブル放送システム。

【請求項 2】 前記特別番組に割り当てられる前記復号情報は、他の前記番組に割り当てられる前記復号情報とは異なることを特徴とする請求項 1 に記載のスクランブル放送システム。

【請求項 3】 複数の前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられることを特徴とする請求項 1 に記載のスクランブル放送システム。

【請求項 4】 複数チャンネルの前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられることを特徴とする請求項 1 に記載のスクランブル放送システム。

【請求項 5】 スクランブルした所定のチャンネルの番組を、視聴者側の受信端末に送信するスクランブル方法において、

スクランブルされた前記番組をデスクランブルするためのスクランブル情報を暗号化し、

暗号化された前記スクランブル情報、および前記番組が特別番組であるか否かを示す番組種別情報を前記番組に付加し、

暗号化された前記スクランブル情報を復号する復号情報、および契約形態に対応する所定の契約情報を出力し、

出力された前記復号情報、および前記契約情報を前記受信端末に供給するか否かを制御することを特徴とするスクランブル方法。

【請求項 6】 前記特別番組に割り当てられる前記復号情報は、他の前記番組に割り当てられる前記復号情報とは異なることを特徴とする請求項 5 に記載のスクランブル方法。

【請求項 7】 複数の前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられることを特徴とする請求項 5 に記載のスクランブル方法。

【請求項 8】 複数チャンネルの前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられることを特徴とする請求項 5 に記載のスクランブル方法。

【請求項 9】 スクランブルした所定のチャンネルの番組を、視聴者側の受信端末に送信するスクランブル装置において、

スクランブルされた前記番組をデスクランブルするためのスクランブル情報を暗号化する暗号化手段と、

暗号化された前記スクランブル情報、および前記番組が特別番組であるか否かを示す番組種別情報を前記番組に付加する付加手段と、

前記暗号化手段により暗号化された前記スクランブル情報を復号する復号情報、および契約形態に対応する所定の契約情報を出力する出力手段と、

前記出力手段からの前記復号情報、および前記契約情報を前記受信端末に供給するか否かを制御する制御手段とを備えることを特徴とするスクランブル装置。

【請求項 10】 前記特別番組に割り当てられる前記復号情報は、他の前記番組に割り当てられる前記復号情報とは異なることを特徴とする請求項 9 に記載のスクランブル装置。

【請求項 11】 複数の前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられることを特徴とする請求項 9 に記載のスクランブル装置。

【請求項 12】 複数チャンネルの前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられることを特徴とする請求項 9 に記載のスクランブル装置。

【請求項 13】 放送供給側から送信されたスクランブ

ルされた所定のチャンネルの番組を、視聴者側の受信端末で受信し、受信した前記番組をデスクランブルするデスクランブル装置において、

前記放送供給側からの前記復号情報、および契約情報を記憶する記憶手段と、

前記放送供給側からの前記番組に付加された前記スクランブル情報を抽出する抽出手段と、

前記スクランブル情報を前記記憶手段に記憶された前記復号情報に基づいて復号する復号手段と、

前記番組のデスクランブルを行うか否かを指示する指示手段と、

前記番組種別情報に基づいて、前記番組が特別番組であるか否かを判定する判定手段と、

前記指示手段による指示内容、前記契約情報、および前記判定手段の判定結果に基づいて、前記番組を前記復号手段により復号された前記スクランブル情報を用いてデスクランブルするか否かを決定する決定手段と前記指示手段によって指示された番組に関する所定の視聴情報を前記放送供給側に提供する提供手段とを備えることを特徴とするデスクランブル装置。

【請求項 1 4】 前記特別番組に割り当てられる前記復号情報は、他の前記番組に割り当てられる前記復号情報とは異なることを特徴とする請求項 1 3 に記載のデスクランブル装置。

【請求項 1 5】 複数の前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられることを特徴とする請求項 1 3 に記載のデスクランブル装置。

【請求項 1 6】 複数チャンネルの前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられることを特徴とする請求項 1 3 に記載のデスクランブル装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、スクランブル放送システム、およびスクランブル方法、並びにスクランブル装置、およびデスクランブル装置に関し、例えば、有料放送システムに用いて好適なスクランブル放送システム、およびスクランブル方法、並びにスクランブル装置、およびデスクランブル装置に関する。

【0002】

【従来の技術】有料放送においては、スクランブル放送と呼ばれる放送方式が用いられることが多い。このスクランブル放送は、放送局側において、元信号を所定の方法で意図的に乱すことにより、放送局と契約していない者が放送を受信しても、正常な画像、音声、およびデータなどを利用することができないようにするものである。すなわち、放送局と契約した者のデコーダに対しては、このスクランブルを解除する鍵信号を与え、この鍵信号によりデコーダがスクランブルされているデータを

元の形にデスクランブルすることで、正常な画像、音声、およびデータなどを得ることができるようにしている。チャンネル単位で契約する場合をフラット、視聴した番組に応じて課金される場合をペイパービューという。ペイパービューのうち、視聴者が急に所定の番組を見なくなった場合でも、所定の操作を行うだけでそれを見ることができる、事前連絡が不要のものを特にインパルスペイパービューという。

【0003】

【発明が解決しようとする課題】有料放送の制御方法としては、昭和 6 3 年度「電気通信技術審議会答申」の「諮問第 1 7 号「放送衛星によるテレビジョン放送における有料方式に関する技術的条件」」がよく知られている。しかしながら、この諮問第 1 7 号答申においては、上記技術的条件の一応の枠組みについては規定されているものの、具体的な制御手順や、インパルスペイパービューの実現方法については規定されていなかった。

【0004】また、例えば、新作映画やタイトルマッチのような高額番組に対して、不正視聴を防ぐための有効な方法や、視聴情報の即時回収などの方法に関しては提案されていない。

【0005】近年、MPEG 2 (Moving Picture Experts Group Phase 2) などによる映像/音声の圧縮手法が確立し、デジタル化した映像/音声信号を少ないビットレートで伝送できるようになってきた。その結果、従来のアナログ放送 1 チャンネル分を伝送していた伝送路によって、マルチチャンネルの映像/音声が多重化されたデジタル放送が実現可能な状況になってきた。

【0006】しかしながら、上記第 1 7 号答申は、従来のアナログ放送を対象に検討されたものであり、マルチチャンネルの制御に適していない部分がある課題があった。

【0007】本発明はこのような状況に鑑みてなされたものであり、視聴契約をしていない番組であっても、簡単な操作で、それをペイパービューで視聴することができるようにし、不正視聴を抑制するとともに、迅速な視聴情報の回収を可能にするものである。

【0008】

【課題を解決するための手段】請求項 1 に記載のスクランブル放送システムは、放送供給側から送信されてきたスクランブルされた所定のチャンネルの番組を、視聴者側の受信端末で受信し、受信した前記番組をデスクランブルするスクランブル放送システムにおいて、放送供給側は、スクランブルされた前記番組をデスクランブルするためのスクランブル情報を暗号化する暗号化手段と、暗号化された前記スクランブル情報、および前記番組が特別番組であるか否かを示す番組種別情報を前記番組に付加する付加手段と、暗号化手段により暗号化された前記スクランブル情報を復号する復号情報、および契約形

態に対応する所定の契約情報を出力する出力手段と、出力手段からの前記復号情報、および前記契約情報を前記受信端末に供給するか否かを制御する制御手段とを備え、受信端末は、放送供給側からの前記復号情報、および契約情報を記憶する記憶手段と、放送供給側からの前記番組に付加された前記スクランブル情報を抽出する抽出手段と、スクランブル情報を前記記憶手段に記憶された前記復号情報に基づいて復号する復号手段と、番組のデスクランブルを行うか否かを指示する指示手段と、番組種別情報に基づいて、前記番組が特別番組であるか否かを判定する判定手段と、指示手段による指示内容、前記契約情報、および前記判定手段の判定結果に基づいて、前記番組を前記復号手段により復号された前記スクランブル情報を用いてデスクランブルするか否かを決定する決定手段と、指示手段によって指示された番組に関する所定の視聴情報を前記放送供給側に提供する提供手段とを備えることを特徴とする。

【0009】特別番組に割り当てられる前記復号情報は、他の前記番組に割り当てられる前記復号情報とは異なるようにすることができる。

【0010】複数の前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられるようにすることができる。

【0011】複数チャンネルの前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられるようにすることができる。

【0012】請求項5に記載のスクランブル方法は、スクランブルした所定のチャンネルの番組を、視聴者側の受信端末に送信するスクランブル方法において、スクランブルされた前記番組をデスクランブルするためのスクランブル情報を暗号化し、暗号化された前記スクランブル情報、および前記番組が特別番組であるか否かを示す番組種別情報を前記番組に付加し、暗号化された前記スクランブル情報を復号する復号情報、および契約形態に対応する所定の契約情報を出力し、出力された前記復号情報、および前記契約情報を前記受信端末に供給するか否かを制御することを特徴とする。

【0013】特別番組に割り当てられる前記復号情報は、他の前記番組に割り当てられる前記復号情報とは異なるようにすることができる。

【0014】複数の前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられるようにすることができる。

【0015】複数チャンネルの前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられるようにすることができる。

【0016】請求項9に記載のスクランブル装置は、スクランブルした所定のチャンネルの番組を、視聴者側の

受信端末に送信するスクランブル装置において、スクランブルされた前記番組をデスクランブルするためのスクランブル情報を暗号化する暗号化手段と、暗号化された前記スクランブル情報、および前記番組が特別番組であるか否かを示す番組種別情報を前記番組に付加する付加手段と、暗号化手段により暗号化された前記スクランブル情報を復号する復号情報、および契約形態に対応する所定の契約情報を出力する出力手段と、出力手段からの前記復号情報、および前記契約情報を前記受信端末に供給するか否かを制御する制御手段とを備えることを特徴とする。

【0017】特別番組に割り当てられる前記復号情報は、他の前記番組に割り当てられる前記復号情報とは異なるようにすることができる。

【0018】複数の前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられるようにすることができる。

【0019】複数チャンネルの前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられるようにすることができる。

【0020】請求項13に記載のデスクランブル装置は、放送供給側から送信されたスクランブルされた所定のチャンネルの番組を、視聴者側の受信端末で受信し、受信した前記番組をデスクランブルするデスクランブル装置において、放送供給側からの前記復号情報、および契約情報を記憶する記憶手段と、放送供給側からの前記番組に付加された前記スクランブル情報を抽出する抽出手段と、スクランブル情報を前記記憶手段に記憶された前記復号情報に基づいて復号する復号手段と、番組のデスクランブルを行うか否かを指示する指示手段と、番組種別情報に基づいて、前記番組が特別番組であるか否かを判定する判定手段と、指示手段による指示内容、前記契約情報、および前記判定手段の判定結果に基づいて、前記番組を前記復号手段により復号された前記スクランブル情報を用いてデスクランブルするか否かを決定する決定手段と、指示手段によって指示された番組に関する所定の視聴情報を前記放送供給側に提供する提供手段とを備えることを特徴とする。

【0021】特別番組に割り当てられる前記復号情報は、他の前記番組に割り当てられる前記復号情報とは異なるようにすることができる。

【0022】複数の前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられるようにすることができる。

【0023】複数チャンネルの前記特別番組に、他の前記番組に割り当てられる前記復号情報とは異なり、かつ共通の前記復号情報が割り当てられるようにすることができる。

【0024】

10

20

30

40

50



【作用】請求項 1 に記載のスクランブル放送システムにおいては、放送供給側においては、暗号化手段により、スクランブルされた番組をデスクランブルするためのスクランブル情報が暗号化され、暗号化されたスクランブル情報、および番組が特別番組であるか否かを示す番組種別情報が、付加手段により番組に付加される。また、制御手段により、出力手段より出力された暗号化されたスクランブル情報を復号する復号情報、および契約形態に対応する所定の契約情報が受信端末に供給されるか否かが制御される。一方、受信端末においては、記憶手段により、放送供給側からの復号情報および契約情報が記憶され、抽出手段により、放送供給側からの番組に付加されたスクランブル情報が抽出され、復号手段により、スクランブル情報が復号情報に基づいて復号される。指示手段により番組のデスクランブルを行うか否かが指示され、判定手段により番組種別情報に基づいて、番組が特別番組であるか否かが判定され、指示手段による指示内容、契約情報、および判定手段の判定結果に基づいて、決定手段により、スクランブル情報を用いて番組をデスクランブルするか否かが決定され、提供手段により、指示手段によって指示された番組に関する所定の視聴情報が放送供給側に提供される。従って、契約形態に拘らず、所定の特別番組を放送し、それをペイパービューで視聴させることができる。

【0025】請求項 5 に記載のスクランブル方法においては、スクランブルされた番組をデスクランブルするためのスクランブル情報が暗号化され、暗号化されたスクランブル情報、および番組が特別番組であるか否かを示す番組種別情報が番組に付加され、暗号化されたスクランブル情報を復号する復号情報、および契約形態に対応する契約情報が出力され、出力された復号情報、および契約情報を受信端末に供給するか否かが制御される。従って、番組によって、復号情報の受信端末への送信方法を変化させることができる。

【0026】請求項 9 に記載のスクランブル装置においては、暗号化手段により、スクランブルされた番組をデスクランブルするためのスクランブル情報が暗号化され、付加手段により、暗号化されたスクランブル情報、および番組が特別番組であるか否かを示す番組種別情報が番組に付加され、出力手段により、スクランブル情報を復号する復号情報、および契約形態に対応する契約情報が出力され、制御手段により、この出力手段からの復号情報、および契約情報を受信端末に供給するか否かが制御される。従って、番組によって、復号情報の受信端末への送信方法を変化させることができる。

【0027】請求項 13 に記載のデスクランブル装置においては、記憶手段により、放送供給側からの復号情報および契約情報が記憶され、抽出手段により、放送供給側からの番組に付加されたスクランブル情報、および番組種別情報が抽出され、復号手段により、スクランブル

情報が復号情報に基づいて復号される。指示手段により番組のデスクランブルを行うか否かが指示され、判定手段により番組種別情報に基づいて、番組が特別番組であるか否かが判定され、指示手段による指示内容、契約情報、および判定手段の判定結果に基づいて、決定手段により、番組がスクランブル情報を用いてデスクランブルされるか否かが決定され、提供手段により、指示手段によって指示された番組に関する所定の視聴情報が放送供給側に提供される。従って、契約形態に拘らず、所定の特別番組をペイパービューで視聴することができる。

【0028】

【実施例】図 1 は、本発明を応用した有料放送システムの一実施例の構成を示すブロック図である。送信側システムのエンコーダ 1 は、映像信号や音声信号をデジタル化し、圧縮するようになされている。多重化器 2（付加手段）は、複数のエンコーダ出力や複数の関連情報を時分割多重する。ここで関連情報とは、番組に関する情報とデスクランブルのためのスクランブル鍵を含む「番組情報」、加入者（視聴者）毎の契約情報（例えばフラットやペイパービューなどの契約形態など）および共通情報の暗号を解くための契約鍵を含む「個別情報」などからなるものとする。

【0029】スクランブラ 3 は、後述する関連情報送出装置 4（暗号化手段）からのスクランブル鍵により、多重化器 2 からの出力信号の所定のものに対して選択的にスクランブルを施すようになされている。

【0030】スクランブル制御システム 6（出力手段、制御手段）は、関連情報送出装置 4 に契約鍵を供給するとともに、受信端末に固有の個別鍵により契約鍵を暗号化し、個別情報の一部として多重化器 2 に供給するようになされている。

【0031】関連情報送出装置 4 は、スクランブラ 3 にスクランブル鍵を供給するとともに、スクランブル制御システム 6 から供給された契約鍵により、スクランブル鍵を暗号化し、共通情報（番組情報）の一部として多重化器 2 に供給するようになされている。

【0032】番組制御システム 5 は、所定の制御信号を発生し、番組に応じてエンコーダ 1 を制御する。すなわち、デジタル化や圧縮の方法を制御する。また、いま、エンコーダ 1 においてエンコードされている番組の番組 ID や対応するチャンネルのチャンネル ID 等を発生し、関連情報送出装置 4 に供給する。視聴情報収集処理システム 7 は、多数の受信端末からアップリンクされる視聴情報（例えば視聴した番組と対応するチャンネル ID、および視聴した時間など）や視聴者からの契約要求を処理し、契約情報としてスクランブル制御システム 6 に供給するようになされている。

【0033】一方、受信端末のデコーダ 8（抽出手段）は、内蔵するデスクランブラにより、後述するセキュリティモジュール 9（記憶手段、判定手段、決定手段、提

供手段) から供給されたスクランブル鍵により、スクランブルされた信号を元の信号にデスクランブルするようになされている。また、番組に付加された個別情報や番組情報を抽出し、出力するようになされている。

【0034】セキュリティモジュール9は、例えばICカード等により構成され、端末固有の個別鍵を記憶し、デコーダ8を介して供給されたスクランブルされていない個別情報を取り込み、個別鍵により個別情報を復号し、契約鍵と契約情報をそれぞれ取り出し、記憶する。また、デコーダ8を介して供給された番組に付随する共

通情報を取り込み、契約鍵により共通情報を復号し、スクランブル鍵を取り出し、デコーダ8に供給するようになされている。

【0035】次にその動作について説明する。まず、送信側システムより受信端末に個別情報が送信される場合の動作について説明する。この個別情報は、図2に示すように、契約鍵に対応する契約鍵番号、契約鍵、契約したチャンネルに対応するチャンネルID、および契約タイプなどを含んでいる。また、個別情報は、送信先の受信端末のID番号に対応する情報も含んでいる。

【0036】契約鍵は、例えば、8ビットの契約鍵番号とともに送信され、複数の契約鍵を使い分けることができるようになっている。契約したチャンネルIDを、例えば16ビットのService\_idで表すものとする。契約タイプは、フラット、ペイパービュー、特別契約を識別することができるもので、例えば4ビットとする。

【0037】この個別情報は、スクランブル制御システム6において、この個別情報が送信されるべき送信先の受信端末に固有の個別鍵を用いて暗号化される。スクランブル制御システム6は、全ての受信端末について、受信端末に固有の個別鍵を受信端末のID番号に対応させて記憶しており、送信先の受信端末のID番号からその個別鍵を検索することができるようになっている。従って、送信先の受信端末のID番号に対応する個別鍵を検索し、それに基づいて、個別情報が暗号化されることになる。暗号化された個別情報は多重化器2に供給される。

【0038】多重化器2においては、エンコーダ1より供給された所定の番組に対応するデジタル化され、圧縮された映像信号や音声信号と、スクランブル制御システム6より供給された個別情報が時分割多重された後、スクランブラ3に供給される。スクランブラ3に供給されたデジタル信号は、関連情報送出装置4より供給されたスクランブル鍵を用いて番組部分だけがスクランブルされ、個別情報の部分はスクランブルされずに伝送路10に送出される。

【0039】なお、この個別情報の受信端末への送信は、個別情報の更新が必要とされる時に、必要に応じて随時行われる。この個別情報には、上述した契約情報が

含まれている。

【0040】次に、通常の番組とそれに付加された番組情報(共通情報の構成要素)が送信側システムから受信端末に送信される場合の動作について説明する。

【0041】番組情報は、例えば図3に示すように、契約タイプ、契約鍵の番号を示す契約鍵番号、暗号化されたスクランブル鍵、チャンネルIDに相当するService\_id、番組を識別するための番組IDなどを含んでいる。また、契約タイプには、特別番組であるかどうかを識別するためのフラグが含まれている。

【0042】関連情報送出装置4において生成された上述したような構成の所定の番組情報は、スクランブル制御システム6より供給された契約鍵によって暗号化された後、多重化器2に供給される。多重化器2においては、エンコーダ1から供給された所定の番組に対応するデジタル化され、圧縮された映像信号や音声信号と、関連情報送出装置4より供給された番組情報が時分割多重され、スクランブラ3に供給される。

【0043】スクランブラ3においては、そこに供給された番組を構成する圧縮された映像信号や音声信号と番組情報が時分割多重されたデジタル信号が、関連情報送出装置4より供給されたスクランブル鍵によって番組部分だけがスクランブルされ、番組情報の部分はスクランブルされずに伝送路10に送出される。

【0044】このようにして、所定の番組とそれに付随する番組情報が送信側システムより受信端末に送信される。

【0045】次に、受信端末側の動作について説明する。

【0046】図4は受信端末において、視聴許可の制御を行う場合の原理的な動作を説明するための図である。デコーダ8は、例えば、デスクランブラ21、第2復号器22(復号手段)、および第1復号器23より構成されている。

【0047】正式に契約した視聴者の受信端末には、個別情報が送信される。送信側システムより、伝送路10を介して送信されたスクランブルされた所定の番組と、スクランブルされていない個別情報が時分割多重されたデジタル信号が、受信端末により受信されると、スクランブルされた番組に対応するデジタル信号は、デスクランブラ21に供給される。

【0048】一方、スクランブルされていない個別情報は、まず、その非暗号部に付加された受信端末のID番号と、セキュリティモジュール9に予め記憶されている受信端末のID番号とが比較され、両者が一致した場合、第1復号器23に供給される。

【0049】第1復号器23に供給された個別情報は、セキュリティモジュール9に記憶されている受信端末に固有の個別鍵によって解読され、契約鍵、および契約情報が取り出され、セキュリティモジュール9に供給さ

れ、記憶される。この契約鍵は、後述する番組情報の解読に使用される。また、契約情報は、受信した番組が契約した番組であるか否かを判断するとき使用される。

【0050】受信端末において、視聴者が番組を視聴しているとき、受信端末は、伝送路10を介して送信されてきたスクランブルされた所定の番組と、それに付随した番組情報を受信している。スクランブルされた所定の番組に対応するデジタル信号は、デスクランブラ21に供給され、それに付随した番組情報は、第2復号器22に供給される。

【0051】所定の番組のチャンネルに対応する契約鍵が、上述したようにして、すでに第1復号器23において復号された個別情報から取り出され、セキュリティモジュール9に記憶されている場合、第2復号器22が動作し、セキュリティモジュール9より供給されたその契約鍵によって番組情報が復号される。番組情報が復号された後、番組情報に含まれたスクランブル鍵が取り出される。

【0052】次に、番組情報は、セキュリティモジュール9により読み込まれ、すでに記憶している契約情報との照合が行われる。その結果、番組情報が付加された番組が、契約した番組であると認識された場合、第2復号器22において得られたスクランブル鍵は、デスクランブラ21に供給される。デスクランブラ21においては、スクランブルされた所定の番組のデジタル信号が、第2復号器22より供給されたスクランブル鍵によってデスクランブルされ、正常に視聴可能な元の信号に戻された後、出力される。

【0053】所定のチャンネルをフラットで契約すると、契約したチャンネルに対応する契約鍵と、そのチャンネルに対応するService\_id、契約タイプ等からなる契約情報を含む個別情報が送信側システムから受信端末に送信され、受信端末を構成するセキュリティモジュール9に記憶される。契約するチャンネル数が多数あれば、上述した手順が繰り返し実行されることになる。

【0054】フラット視聴の場合、受信した番組に付随する番組情報内のService\_idがセキュリティモジュール9に記憶されており、かつ番組情報内の契約鍵番号で示される契約鍵がセキュリティモジュール9に記憶されており、かつService\_idに対応する契約タイプがフラットである場合、第2復号器22によって、番組情報が復号され、得られたスクランブル鍵がデスクランブラ21に供給され、デスクランブラ21が動作する。これにより、所定の番組が正常にデスクランブルされた映像および音声を得られ、その番組の視聴が可能となる。

【0055】ペイパービュー契約の場合、契約すると、契約したチャンネルに対応する契約鍵と、そのチャンネルに対応するService\_id、契約タイプを含む

個別情報が送信側システムから受信端末に送信され、デコーダ8を介してセキュリティモジュール9に供給され、記憶される。契約するチャンネルが多数ある場合、この手順が繰り返されることになる。

【0056】フラットで契約していても、高額の特別番組を視聴するときに、ペイパービューの操作をすることによって視聴が可能となるようにする場合、送信側システムから、受信端末に特別番組の視聴許可に、契約鍵、特別番組のチャンネルに対応するService\_id、特別契約を示す契約タイプを含む個別情報が送信される。この個別情報は、セキュリティモジュール9に供給され、記憶される。特別番組が多数あり、それぞれに個別の契約鍵を割り当てる場合には、この手順が繰り返されることになる。

【0057】高額の特別番組は、視聴料の速やかな請求や、視聴率の速やかな収集が番組供給者から望まれている場合が多い。通常のペイパービュー方式では、例えば、月毎の定期的な視聴情報を受信端末側のセキュリティモジュール9から収集し、その結果から毎月のペイパービュー料金を算出するようになっている。従って、特別番組の視聴料金を速やかに収集することができない。

【0058】そこで、電話連絡、または受信端末を操作することにより、所定の特別番組の視聴を希望することを送信側システムに対して事前に連絡を行った視聴者に対してだけ、予め、この特別番組に対応する契約鍵を送信するようにする。これにより、事前連絡を行った視聴者は、ペイパービューの場合と同様の操作を行うことで、特別番組を視聴することが可能になる。この場合、送信側システムは、事前連絡をしてきた視聴者を認識しているので、視聴率の把握を迅速に行ったり、これらの者に対する課金処理を速やかに実施することが可能である。また、事前連絡を行った視聴者だけに契約鍵が送信されるので、契約鍵が不正解読される可能性を減少させることができる。

【0059】一方、事前連絡を行っていない視聴者は、特別番組を視聴するための契約鍵を送信側システムから受け取っていないので、特別番組を視聴することはできない。

【0060】また、特別番組の視聴を事前連絡により申し込んだ場合でも、番組開始前であれば、送信側システムに連絡することにより、キャンセルすることができ。例えば、視聴者が電話連絡または受信端末を操作することにより、送信側システムに所定の特別番組の視聴の申し込みのキャンセルを連絡すると、送信側システムは、視聴者からのこの連絡に基づいて、特別番組用の契約鍵を消去するために、所定の情報を含めた個別情報を再度視聴者側の受信端末に伝送路10を介して送信する。

【0061】例えば、個別情報の中に予約のキャンセルを示す専用のフラグを用意するようにしてもよいが、個

10

20

30

40

50

別情報の中の契約鍵に値000000000000000000(16進数)を設定し、これをキャンセル用に割り当てて使用することも可能である。この場合、送信側システムは、図5に示したような個別情報を受信端末に送信することになる。受信端末は、送信側システムからの個別情報を受信すると、その中の契約鍵に設定された値が000000000000000000(16進数)であることを認識し、契約鍵番号に対応する所定の番組の視聴が視聴者によってキャンセルされたことを認識するとともに、すでにセキュリティモジュール9内に記憶してある、その契約鍵番号、およびそれに対応する契約鍵を消去する。

【0062】これにより、特別番組が送信されてきた場合でも、特別番組とともに送信されてくる番組情報の中の契約鍵番号、およびそれに対応する契約鍵がセキュリティモジュール9に存在しないことになり、視聴者の受信端末はこの特別番組をデスクランブルすることができず、視聴者は特別番組を視聴することができなくなる。

【0063】所定の番組の視聴を申し込む事前連絡が多数の視聴者から同時刻に送信側システムに要求されると、送信側システムの受付処理が番組の開始時刻までに間に合わなくなる恐れがある。また、このように番組開始直前に申し込みが多数発生すると、短時間に多数の個別情報を送信する必要が生じ、番組の開始時刻に間に合わなくなる恐れがある。

【0064】そこで、事前連絡を行った視聴者だけでなく、それ以外の視聴者にも、すなわち、全ての視聴者に対して、予め、特別番組の契約鍵を個別情報に含ませて前もって送信しておくようにする。この個別情報を受信した受信端末は、特別番組の契約鍵をその契約鍵番号とともにセキュリティモジュール9に記憶させる。従って、特別番組を受信した全ての受信端末は、この特別番組の契約鍵番号に対応する契約鍵をすでにセキュリティモジュール9内に記憶していることになる。

【0065】一方、受信端末側では、視聴者が受信端末を操作することにより、事前連絡を行った場合、事前連絡を行ったという情報を、申請したチャンネルIDと番組IDとともに、セキュリティモジュール9内に記憶しておくようにする。特別番組を受信すると、受信端末は、それが特別番組であることを特別番組とともに送信されてきた番組情報の中の契約タイプによって認識する。この場合、特別番組の契約鍵番号に対応する契約鍵がすでにセキュリティモジュール9内に記憶されているが、受信端末は、特別番組である場合、事前連絡を行ったという情報とともに記憶されているチャンネルID、および番組IDが、番組情報内のService\_id、および番組IDとそれぞれ一致するか否かを判定し、一致した場合にのみ、送信されてきた特別番組をデスクランブルするために、デスクランブラ21に番組情報内のスクランブル鍵を供給する。これにより、事前連

絡を行った視聴者だけが特別番組を視聴することができるようになる。

【0066】これにより、仮に番組開始直前に申し込みが殺到したとしても、短時間に多数の個別情報を受信端末に送信する必要がなくなり、番組の開始時刻に間に合わなくなるといった不都合をなくすることができる。また、事前連絡を行った視聴者に対する速やかな課金処理を行うことが可能である。

【0067】ここで、視聴者が番組の視聴の予約をキャンセルした場合、すなわち、受信端末を操作することにより、所定の番組の予約のキャンセルを指示した場合、受信端末は、予約キャンセルに対応する所定の信号を送信側システムに電話回線11を介して送信するとともに、セキュリティモジュール9内にすでに記憶されている予約した番組のチャンネルID、および番組IDを消去する。これにより、受信端末は、予約をキャンセルした番組の視聴が不可能となる。

【0068】マルチチャンネルのデジタル放送においては、上述したような特別番組が多数存在した場合、それぞれ互いに異なる別々の契約鍵を割り当てるようにすることも可能であるが、その場合、送信側システムから受信端末に送信される個別情報数が増加する。そこで、複数の特別番組に共通の契約鍵を使用するようにすることにより、受信端末に送信される個別情報数の増大を抑制することができる。また、必要な個別情報が全てセキュリティモジュール9内に取り込まれ、記憶されるまでに要する時間をより短くすることが可能である。

【0069】また、複数のチャンネル間においても、複数の特別番組に共通の契約鍵を割り当てるようにすることにより、個別情報数の増大を抑制することができる。この場合、チャンネルIDを特定することができないので、契約鍵とともに送信するService\_idには不特定を示す例えば値0000(16進数)を割り当てるようにする。受信端末側では、Service\_idに値0000(16進数)が設定された契約鍵を、チャンネルIDに拘らず、対応する契約鍵番号の特別番組に対して使用する。

【0070】予め、必要な個別情報が全ての受信端末のセキュリティモジュール9に取り込まれ、記憶された後で、番組を視聴することができるようになるが、その流れは視聴形態によりいくつかの場合がある。上述したように、番組に付随して送信される番組情報には、暗号化されたスクランブル鍵、それに対応する契約鍵の番号を示す契約鍵番号、チャンネルIDに対応するService\_id、および特別番組であるか否かを識別するためのフラグ(契約タイプに含まれる)が含まれている。

【0071】次に、視聴形態に応じて、スクランブル鍵を復号する契約鍵を伝送する形態を変化させて、視聴制御を行う方法について説明する。

【0072】フラット視聴の場合、受信した番組に付随

する番組情報内の `Service_id` がセキュリティモジュール 9 内に記憶されており、かつ番組情報内の契約鍵番号で示される契約鍵がセキュリティモジュール 9 内に記憶されており、かつ `Service_id` に対応する契約タイプがフラットであるとき、スクランブル鍵を復号してデスクランブラ 21 に供給し、デスクランブラ 21 を動作させる。デスクランブラ 21 においては、送信システムより供給された所定の番組に対応するスクランブルされた映像／音声信号をデスクランブルし、元の映像／音声信号を得て、番組の視聴を可能とする。

【0073】ペイパービュー視聴の場合、受信した番組に付随する番組情報内の `Service_id` がセキュリティモジュール 9 内に記憶されており、かつ番組情報内の契約鍵番号で示される契約鍵がセキュリティモジュール 9 内に記憶されており、かつ `Service_id` に対応する契約タイプがペイパービューのとき、例えば受信端末に設けられた「ペイ確認」ボタン 12（指示手段）を押すなどのペイパービュー操作を行うことにより、番組の視聴を可能とすることができる。

【0074】ペイパービュー操作が行われると、例えば視聴した番組のチャンネル ID、番組 ID、および視聴時間などからなる視聴履歴が、その都度セキュリティモジュール 9 に記憶される。セキュリティモジュール 9 に記憶された視聴情報は、所定の周期で、例えば 1 カ月毎に送信側システムに電話回線 11 を介して送信される。送信側システムは、受信端末から送信されてきた視聴情報に基づいて、各受信端末毎の課金処理を行う。

【0075】特別番組視聴の場合、受信した番組に付随する番組情報内の `Service_id` が、セキュリティモジュール 9 内に記憶されており、かつ番組情報内の契約鍵番号で示される契約鍵がセキュリティモジュール 9 内に記憶されており、かつ番組情報内の契約タイプによって特別番組であることが示されているとき、すなわち、特別番組であることを示すフラグが立っているとき、上述したペイパービューの場合と同様の操作を行うことにより、特別番組の視聴を可能とすることができる。この場合、送信側システムから個別情報によって、特別番組に対応する `Service_id`、契約鍵番号、およびそれに対応する契約鍵が受信端末に送信され、セキュリティモジュール 9 にすでに記憶されている。

【0076】このように、事前連絡がなくても、ペイパービューの場合と同様の操作を行うことにより、特別番組の視聴を可能とすることができる。この場合、視聴履歴は通常のペイパービューの場合と同様に、所定の周期で、例えば 1 カ月毎に送信側システムに送信される。従って、この場合、送信側システムは、特別番組であっても、通常の番組と同様に所定の周期で課金処理を行うことになる。

【0077】また、事前連絡がないとき、特別番組を視

聴させないように運用する場合、受信端末においては、受信した特別番組に付随した番組情報内のチャンネル ID、および番組 ID が、セキュリティモジュール 9 内に記憶されているチャンネル ID、および番組 ID とそれぞれ一致するか否かが判定され、一致しないと判定された場合、番組情報に含まれるスクランブル鍵をデスクランブラ 21 に供給しないように制御される。その結果、この特別番組を視聴することができなくなる。

【0078】一方、受信した特別番組に付随した番組情報内のチャンネル ID、および番組 ID が、セキュリティモジュール 9 内に記憶されているチャンネル ID、および番組 ID とそれぞれ一致すると判定された場合、番組情報に含まれるスクランブル鍵をデスクランブラ 21 に供給するように制御される。その結果、この特別番組を視聴することが可能となる。

【0079】ここで、セキュリティモジュール 9 内に記憶されているチャンネル ID、および番組 ID は、視聴者が受信端末を操作することにより、所定の特別番組の視聴の予約を事前申請したときに記憶されたものである。そのとき、この事前申請に対応する信号は、送信側システムにも送信される。従って、送信側システムにおいては、事前連絡者に対する速やかな課金処理を実施することが可能である。

【0080】複数チャンネルで特別番組用の契約鍵を共有する場合、上述した特別番組視聴は、受信端末が受信した番組に付随する番組情報内の `Service_id` がセキュリティモジュール 9 内に記憶されていないが、番組情報内の契約鍵番号に対応する契約鍵がセキュリティモジュール 9 内に記憶されており、かつ番組情報内の契約タイプに特別番組であることを示すフラグが立っているとき、ペイパービューの場合と同様の操作を行うことにより、特別番組の視聴が可能となる。

【0081】以上のように、本発明によれば、契約鍵、`Service_id`、契約タイプの送出形態により、フラット、インパルスペイパービュー、特別番組、および事前申し込み者に対してだけ視聴を可能にするコール Ahead ペイパービューの制御を統一的行うことが可能となる。

【0082】なお、上記実施例においては、個別情報を放送電波によって受信端末に供給するようにしたが、電話線を介して送信したり、IC カード、その他の記録媒体によって、受信端末に供給するようにすることも可能である。

【0083】また、上記実施例においては、伝送路 10 を放送波であるものとして説明したが、これに限定されるものではなく、光ファイバケーブルやその他の伝送媒体とすることも可能である。

【0084】さらに、上記実施例においては、例として、契約タイプに 4 ビット、契約鍵番号に 8 ビット、契約鍵およびスクランブル鍵に 64 ビット、`Service`

e \_ i d および番組 I D に 1 6 ビットをそれぞれ割り当てようとしたが、これに限定されるものではなく、他の任意のビット数をそれぞれ割り当てるようにすることが可能である。

#### 【 0 0 8 5 】

【発明の効果】請求項 1 に記載のスクランブル放送システムによれば、放送供給側においては、暗号化手段により、スクランブルされた番組をデスクランブルするためのスクランブル情報が暗号化され、暗号化されたスクランブル情報、および番組が特別番組であるか否かを示す番組種別情報が、付加手段により番組に付加される。また、制御手段により、暗号化されたスクランブル情報を復号する復号情報、および契約形態に対応する所定の契約情報を受信端末に供給するか否かが制御される。一方、受信端末においては、抽出手段により、放送供給側からの番組に付加されたスクランブル情報が抽出され、復号手段により、スクランブル情報が復号情報に基づいて復号される。指示手段により番組のデスクランブルを行うか否かが指示され、判定手段により番組種別情報に基づいて、番組が特別番組であるか否かが判定され、指示手段による指示内容、契約情報、および判定手段の判定結果に基づいて、決定手段により、スクランブル情報を用いて番組をデスクランブルするか否かが決定され、提供手段により、指示手段によって指示された番組に関する情報が放送供給側に提供されるようにしたので、契約形態に拘らず、所定の特別番組を放送し、それをペーパービューで視聴させることができる。また、前もって番組の視聴を予約させることにより、放送供給側は視聴情報を迅速に回収することができる。また、復号情報を番組の視聴を予約した者にだけ供給することにより、不正視聴を抑制することが可能となる。

【 0 0 8 6 】請求項 5 に記載のスクランブル方法、および請求項 9 に記載のスクランブル装置によれば、スクランブルされた番組をデスクランブルするためのスクランブル情報が暗号化され、暗号化されたスクランブル情報、および番組が特別番組であるか否かを示す番組種別情報が番組に付加され、暗号化されたスクランブル情報を復号する復号情報、および契約形態に対応する所定の契約情報を受信端末に供給するか否かが制御されるようにしたので、番組によって、復号情報の受信端末への送信方法を変化させることができる。従って、前もって番組の視聴を予約した者にだけその番組の復号情報を供給することができる。これにより、不正視聴を抑制するこ

とが可能となる。

【 0 0 8 7 】請求項 1 3 に記載のデスクランブル装置によれば、抽出手段により、放送供給側からの番組に付加されたスクランブル情報が抽出され、指示手段により番組のデスクランブルを行うか否かが指示され、判定手段により番組種別情報に基づいて、番組が特別番組であるか否かが判定され、指示手段による指示内容、契約情報、および判定手段の判定結果に基づいて、決定手段により、番組を復号情報により復号されたスクランブル情報を用いてデスクランブルするか否かが決定され、提供手段により、指示手段によって指示された番組に関する所定の視聴情報が放送供給側に提供されるようにしたので、契約形態に拘らず、所定の特別番組をペーパービューで視聴することができる。また、前もって番組の視聴を予約させることにより、放送供給側に視聴情報を迅速に提供することができる。また、番組の視聴を予約した者にだけ復号情報が供給されるようにすることにより、不正視聴を抑制することが可能となる。

#### 【図面の簡単な説明】

【図 1】本発明を応用した有料放送システムの構成例を示すブロック図である。

【図 2】個別情報の一部を示す図である。

【図 3】番組情報の一部を示す図である。

【図 4】受信端末の動作の原理を説明するための図である。

【図 5】番組をキャンセルした場合に送信される個別情報の一部を示す図である。

#### 【符号の説明】

- 1 エンコーダ
- 2 多重化器（付加手段）
- 3 スクランブラ
- 4 関連情報送出装置（暗号化手段）
- 5 番組制御システム
- 6 スクランブル制御システム（出力手段、制御手段）
- 7 視聴情報収集処理システム
- 8 デコーダ（抽出手段）
- 9 セキュリティモジュール（記憶手段、判定手段、決定手段、提供手段）
- 10 伝送路
- 11 電話回線
- 21 デスクランブラ（指示手段）
- 22 第 2 復号器
- 23 第 1 復号器

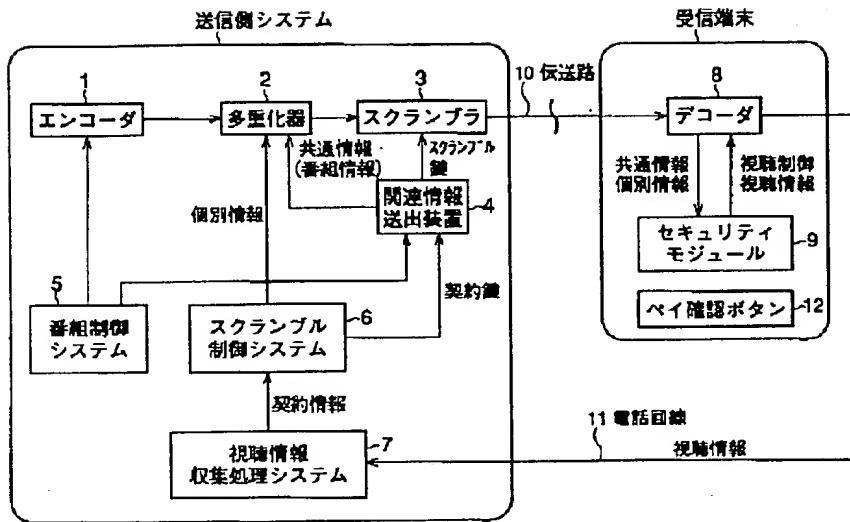
【図 2】

契約番号	契約番号	service_id	契約番号
8ビット	64ビット	16ビット	4ビット

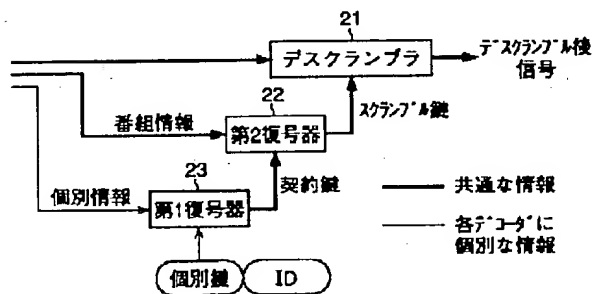
【図 3】

契約番号	契約番号	スクランブル鍵(暗号化)	service_id	番組ID
4ビット	8ビット	64ビット	16ビット	16ビット

【図 1】



【図 4】



【図 5】

契約鍵 番号	契約鍵 (0x0000000000000000)	service_id	契約 鍵
8ビット	64ビット	16ビット	4ビット

フロントページの続き

(72)発明者 井原 喜一

東京都品川区北品川 6 丁目 7 番 3 5 号 ソ

ニー株式会社内

This Page Blank (uspto)